Int. J. on Recent Trends in Engineering and Technology, Vol. 10, No. 2, Jan 2014

Robust Watermarking Technique using 2D Logistic Map and Elliptic Curve Cryptosystem in Wavelets

Chittaranjan Pradhan[1], Bidyut Jyoti Saha[2], Kunal Kumar Kabi[3], Ajay Kumar Bisoi[4]
School of Computer Engineering, KIIT University, Bhubaneswar, India
[1]chitaprakash@gmail.com, [2]bidyutjyotisaha@gmail.com
[3]kunal.kabi90@gmail.com, [4]akbisoifcs@kiit.ac.in

Abstract— **Copyright protection is a vital issue in modern day's data transmission over internet. For copyright protection, watermarking technique is extensively used. In this paper, we have proposed a robust watermarking scheme using 2D Logistic map and elliptic curve cryptosystem (ECC) in the DWT domain. The combined encryption has been taken to enhance the security of the watermark before the embedding phase. The PSNR value shows the difference between original cover and embedded cover is minimal. Similarly, NC values show the robustness and resistance capability of the proposed technique from the common attacks such as scaling, Gaussian noise etc. Thus, this combined version of 2D Logistic map and Elliptic curve cryptosystem can be used in case of higher security requirement of the watermark signal.**

Index Terms— **watermarking, 2D logistic map, elliptic curve cryptosystem, wavelet, embedding, extraction.**

I. INTRODUCTION

Digital watermarking is the primary technique to deal with the data piracy and to verify the ownership of the author. Though there are different types of watermarking techniques available, robust watermarking is the technique which can resist the common attacks like JPEG compression, Gaussian noise, scaling etc. That means in case of such attacks, the watermark can still be extracted and identified [1, 2].

Encryption techniques such as DES, AES and RSA can be used for the watermark before the embedment into the cover to provide the security to the watermark. As asymmetric key cryptography is more secure than the symmetric key cryptography, our focus is on the former one. The key size of the asymmetric key cryptography is a big problem, which has to be given importance at the encryption time [3].

Although RSA and ElGamal are secure asymmetric-key cryptosystems, their security comes with a price, i.e. their large keys. Researchers have looked for alternatives that give the same level of security with smaller key sizes. One of the promising alternative is the elliptic curve cryptosystem (ECC).This system is based on the theory of elliptic curves. It was proven that to achieve reasonable security, a 1024-bit modulus would have to be used in a RSA cryptosystem, while 160-bit modulus should be sufficient for ECC. Thus, in the late 1990s, elliptic curve systems started receiving commercial acceptance [4].

In 2009, Hongbin Kong et. al proposed a hybrid model to encrypt ontology using both elliptic curve cryptosystem and digital watermark. Elliptic curve cryptosystem provides greater security and more efficient performance than the common asymmetric key techniques like RSA [5]. In 2010, Youssef Zaz et. al proposed a novel method to embed Electronic Patient Records (EPR) data in medical images. After liberating a zone by compressing the image Least Significant Bit plan using Huffman coding, the EPR is encrypted by

DOI: 01.IJRTET.10.2.34

an elliptic curve cryptosystem (ECC) and inserted into this zone [4]. Similarly Guiliang Zhu et. al have worked on digital image encryption algorithm based on pixels in 2010 [6]. The approach they have followed is scrambling the image pixels, then using the method of watermark and at last, choosing a camouflaged image to vision or the pixels of the true image, getting the final encryption image. The key parameters are encrypted by elliptic curve cryptosystem (ECC).

Motivated by the dual encryption process [7, 8], here, we have worked on the combined version of 2D logistic map and ECC algorithm for the watermark encryption. ECC has been chosen for the better key manageable algorithm. For the robustness, DWT has been taken as the domain.

II. BACKGROUND

In this paper, we propose an algorithm for robust and secure watermarking using the combined version of 2D logistic map and ECC technique in the DWT domain. The different techniques used are:

A. 2D Logistic Map

The 2D logistic map is an extension of 1D logistic map. It increases the key space as well as the dependency on control parameters. In 2D logistic map, it is bit harder to guess the secret information. It also exhibits greater amount of chaotic behavior on the generation of sequence [9]. In overall, it increases the complexity of the algorithm. The 2D logistic map F(m, n) is defined as:

$$F(m,n)=\begin{cases} M_{i+1}=\alpha_1 M_i(1-M_i)+\beta_1 N_i^2 \\ N_{i+1}=\alpha_2 N_i(1-N_i)+\beta_2(M_i^2+M_i N_i) \end{cases} \quad (1)$$

where, i= 0, 1, 2… Here, $\alpha_1,\beta_1,\alpha_2,\beta_2$ are system control parameters. M_0 and N_0 are initial conditions. The equation generates sequence in the range of 0 and 1with chaotic behavior 2.75 < $\alpha_1 \le 3.4$, 0.15 < $\beta_1 \le 0.21$, 2.7 < $\alpha_2 \le 3.45$, 0.13 < $\beta_2 \le 0.15$ and the values of M_i and N_i lies in (0, 1) [9].

B. Elliptic Curve Cryptosystem (ECC)

Elliptic curves are cubic equations in two variables that are similar to the equations used to calculate the length of a curve in the circumference of an ellipse [10]. The general equation for an elliptic curve is:

$$y^2+b_1xy+b_2y=x^3+a_1x^2+a_2x+a_3 \quad (2)$$

Elliptical curves over real numbers use a special class of elliptic curves $E_p(a,b)$ of the form: $y^2=x^3+ax+b$, where a, b are in whatever is the appropriate set (rational numbers, complex numbers, integers mod n, etc).

In the above equation, if $4a^3+27b^2\neq 0$, the equation represents a nonsingular elliptic curve; otherwise, the equation represented a singular elliptic curve. In a nonsingular elliptic curve, the equation $x^3+ax+b=0$ has three distinct roots (real or complex); in a singular curve the equation $x^3+ax+b=0$ does not have three distinct roots [10].

Looking at the equation, we can see that left hand side has a degree of 2 while the right hand side has a degree of 3. This means that a horizontal line can intersects the curve in three points if all the roots are real. However, a vertical line can intersects the curve at most in two points. The specific properties of a nonsingular elliptic curve allow us to define an addition operation on the operation on the points of the curve.

C. Discrete Wavelet Transform (DWT)

The watermark can be embedded in spatial or frequency domain. But, frequency domain watermarking is more robust than the spatial domain. DWT is the most common technique used to convert the image into the frequency domain [7].

The DWT is computed by successive low pass and high pass filtering of the discrete time domain signal. The image after wavelet decomposition is divided into four bands in horizontal direction, vertical direction, diagonal direction and low frequency part which can be further decomposed.

According to Discrete wavelets theory and human visual characteristics, the embedding capacity will decrease with the increase of layer numbers. The high frequency part of discrete wavelets represent the edge, outline and texture information and other detail information. Embedded watermark is difficult to be detected

in these parts, but it is easy to be destroyed and has a poor stability after image processing. The low frequency part concentrates on most of the energy of image, whose amplitude of coefficient is larger than the other parts. Most of the common attacks to low frequency coefficients are almost invariant. Still, there are some attacks like low pass filtering, which can affect the low frequency coefficients to destroy the host image. Thus, it is better to embed watermark in medium frequency domain [7].

D. Performance Analysis

The performance of the watermarked image can be evaluated on the basis of peak signal to noise ratio (PSNR) in decibels (dB). Higher the value of PSNR better is the quality of the watermarked image [7, 8].

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2 \tag{3}$$

$$PSNR = 10\log_{10}\left(\frac{R}{MSE}\right) \tag{4}$$

where, MSE is the mean square error of the watermarked image and the original image and m, n are the number of rows and number of columns. I and K are the original and watermarked image respectively. There may be some attacks applied to the cover image. The quality of the extracted watermark is evaluated using Normalized cross-correlation (NC) formula as:

$$NC = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} w(i,j) * w^{'}(i,j)}{\sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} w(i,j)^2}\ \sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} w^{'}(i,j)^2}} \tag{5}$$

The ideal value of the NC is 1 which means the original and the extracted watermarks are exactly of the same quality [7].

III. Proposed Algorithms

A. Watermarking using Elliptical Curve Cryptosystem (ECC)

Here, each plaintext is mapped with the points in the Elliptical curve for simulation. An algorithm has been proposed to find one to one correspondence between symbols (or a block of text) and the points on the graph. Let X be the original image of size $N \times N$ and w be the watermarking image with size $M \times M$. Normally, $N = 2K \times M, K \geq 0.5$ i.e. the size of watermark is smaller than or equal to that of the original image.

Embedding Scheme: The different steps of embedding scheme of the proposed algorithm are:

1. Owner encrypts the watermark w using 2D logistic map to w'.
2. The encrypted watermark w' is further encrypted with the ECC to produce w''.
3. Make three-level wavelet decomposition to the original image X and use the medium frequencies $HL3$ as the embedded domain, the wavelet coefficients are extracted as $CA3$.
4. Do one-level wavelet decomposition to the modified watermark w'' and extract the frequency coefficients $cw1$.
5. Embed the watermark into original image using the following equation:

$$CA3^{'}(i,j) = CA3(i,j) + \alpha * CA3(i,j) * cw1(i,j) \tag{6}$$

Where α stands for the watermarking strength, whose value lies in between visibility and robustness. Lower the value of α, better for the quality of the watermarked image.

6. Make a wavelet reconstruction of the embedded datum to produce the embedded image X'.

The pictorial representation of the embedding process is shown in Figure 1:

Extraction Scheme: The watermark extraction scheme is the reverse process of embedding scheme. As it is a non blind scheme, the original image is required at the recovery time. The detailed steps are:

1. Make three-level wavelet decomposition to the watermarked image, the wavelet coefficients of $HL3$ are extracted as $CA3'$.

2. Do three-level wavelet decomposition to the original image X and extract the wavelet coefficients as $CA3''$.
3. The watermark frequency coefficients $cw1'$ are extracted by applying the equation below:

$$cw1^{'}(i,j) = \left[CA3^{'}(i,j) \big/ CA3^{''}(i,j) - 1 \right] \big/ \alpha \quad (7)$$

4. Use one-level wavelet transformation to reconstruct the watermark.
5. The owner uses ECC to decrypt the extracted watermark to w'.
6. 2D logistic map is used to generate the watermark w.

The pictorial representation of the extraction process is shown in Figure 2:

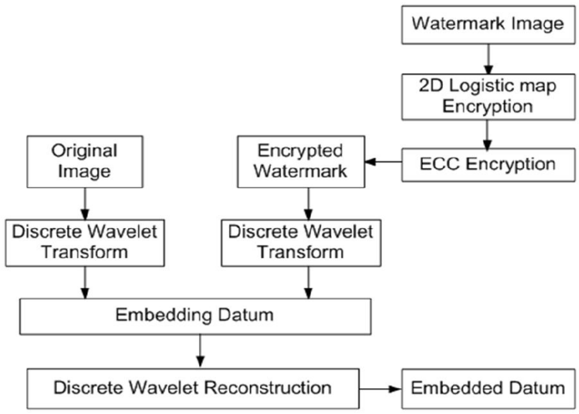

Figure 1. Embedding process using ECC

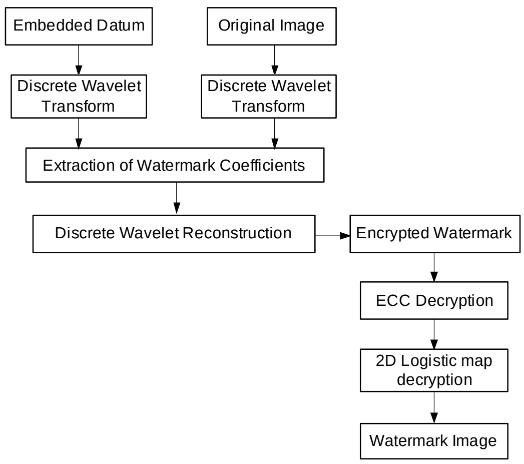

Figure 2. Extraction process using ECC

Result Analysis: For the experimental results, we have taken lena64.bmp as the watermark image of size 64×64. Similarly, baboon.bmp has been taken as the cover of size 512×512. Figure 3(b) shows the encrypted watermark after the encryption using 2D logistic map. The parameters taken for this are: α_1=2.93, α_2=2.97, β_1= 0.17, β_2 = 0.14, M_0 = 0.32 and N_0 = 0.62. For every value of the watermark image, we get a point in the elliptical curve. The points are stored and we get an encrypted watermark image shown in Figure 3(c). Here, we have taken ***p*** (modulo) = 257 and a=25 and b=35. The embedded cover is shown in Figure 3(e). When the extraction process is applied to the embedded cover, we have got the image as shown in Figure 3(f). Now while decrypting the encrypted image we calculated the original values of the watermark from the points of the elliptical curve and thus watermark is recovered as shown in Figure 3(g). When, this image is decrypted by 2D logistic map, the watermark message is recovered as shown in Figure 3(h).

Here, the PSNR value found is +71.57dB. The encryption time and decryption time of this process are 6.2813 sec and 3.1406 sec respectively. Table I shows the results of NC values with respect to different attacks. From the results, it can be seen that though the image quality degrades with different types of attacks; still the watermark can be extracted.

TABLE I. NC VALUES USING ECC

JPEG Compression	Scaling	Gaussian Noise
0.9745	0.9840	0.9925

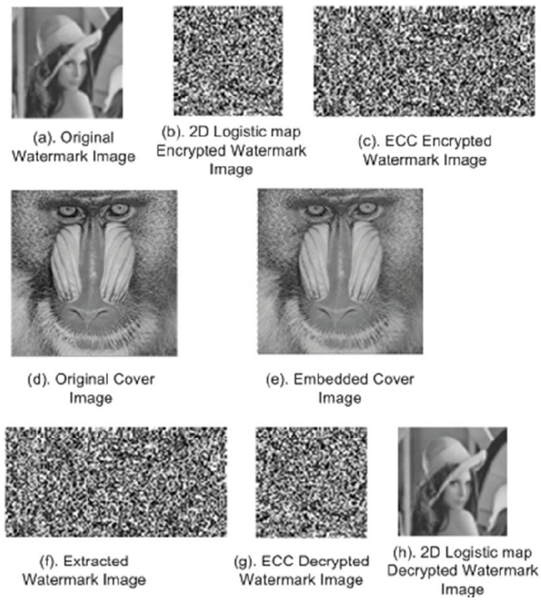

Figure 3. Results using ECC

B. Watermarking using Elliptical Curve cryptosystem (ECC) Simulating ElGamal

The security of the above proposed approach can further be enhanced by encrypting the elliptic curves. The common one is to simulate the ElGamal cryptosystem using an elliptic curve over $GF(\rho)$ or $GF(2^n)$:

Generating Public and Private Keys: The keys can be generated as:

1. Bob chooses $\mathrm{E}(a,\ b)$ with an elliptic curve over $GF(\rho)$ or $GF(2^n)$.
2. Bob chooses a point on the curve $e_1(x_1, y_1)$.
3. Bob chooses an integer d.
4. Bob calculates $e_2(x_2, y_2) = d * e_1(x_1, y_1)$. Multiplication here means multiple addition of points as defined before.
5. Bob announces $\mathrm{E}(a,\ b)$, $e_1(x_1, y_1)$ and $e_2(x_2, y_2)$ as his public key; he keeps d as his private key.

Encryption: Alice selects P, a point on the curve, as her plaintext, P. She then calculates a pair of points on the text as cipher texts:

$$C_1 = r * e_1 \tag{8}$$

$$C_2 = P + r * e_2 \tag{9}$$

Decryption: Bob, after receiving C_1 and C_2, calculates P, the plaintext using the formula:

$$P = c_2 - (d * c_1) \tag{10}$$

Where, minus sign indicates addition with the inverse.

We can prove that the P calculated by Bob is the same as intended by Alice, as shown below:

$$P + r*e_2 - (d*r*e_1) = P + (r*d*e_1) - (d*r*e_1) = P + 0 = P \qquad (11)$$

$P, C_1, C_2, e_1 and e_2$ are all points on the curve. The result of adding two inverse points on the curve is the zero point.

Embedding Scheme: The embedding scheme is similar to the previous approach. Instead of the normal ECC, ECC simulating ElGamal has been taken for encrypting the 2D logistic map encrypted watermark. The pictorial representation of the embedding is shown in Figure 4.

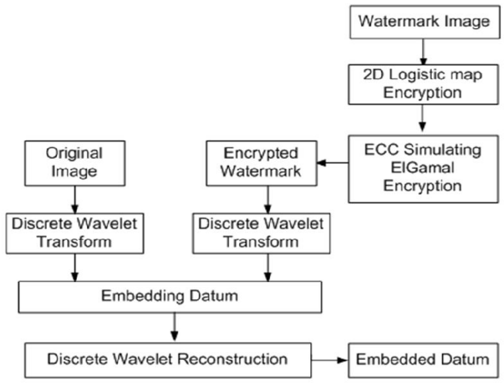

Figure 4. Embedding process using ECC simulating ElGamal

*Extraction Scheme:*The extraction scheme is also similar to the previous approach. Here, instead of normal ECC, we have used the ECC simulation ElGamal version for the encryption purpose. Figure 5 shows the detailed of this.

Result Analysis: For the experimental results, we have taken the same watermark and cover images. Figure 6(b) shows the encrypted watermark after the encryption using 2D logistic map. The parameters taken for this are: α1=2.93, α2=2.97, β1= 0.17, β2 = 0.14, M_0 = 0.32, N_0 = 0.62. Figure 6(c) shows the encrypted watermark after encryption using ECC simulating ElGamal. For getting larger prime numbers, we have scaled the watermark for storing the values of C2(x, y) and C1(x, y). Here, we have taken ***p*** (modulo) = 257 and a=25, b=35, x=242, y=59, d=14 and r=16. The embedded cover is shown in Figure 6(e). When the extraction process is applied to the embedded cover, we have got the image as shown in Figure 6(f). Now, the extracted watermark is decrypted using Bob's private keys, which is shown in Figure 6(g). When, this image is decrypted by 2D logistic map, the watermark message is recovered as shown in Figure 6(h).

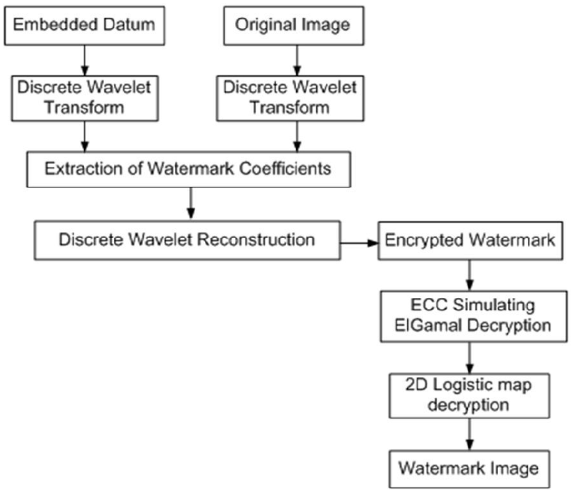

Figure 5. Extraction process using ECC simulating ElGamal

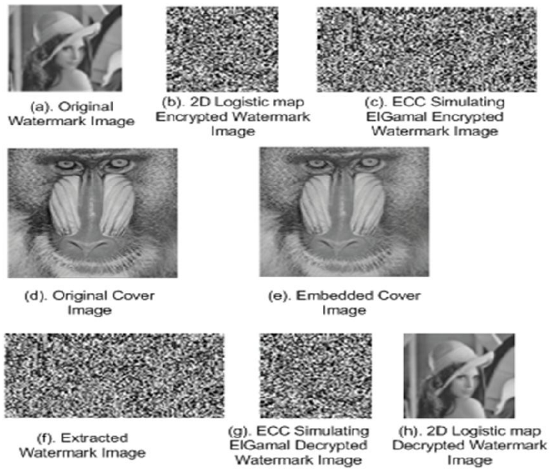

Figure 6. Results using ECC simulating ElGamal

Here, the PSNR values found is +68.42dB. The encryption time and decryption time of this process are 10.9844 sec and 5.9375 sec respectively. Table II shows the results of NC values with respect to different attacks. From the results, it can be seen that though, the image quality degrades with different types of attacks; still the watermark can be extracted.

TABLE II. NC VALUES USING ECC SIMULATING ELGAMAL

JPEG Compression	Scaling	Gaussian Noise
0.9565	0.9645	0.9875

IV. CONCLUSIONS

In the proposed algorithm, we have used the combined version of 2D logistic map and elliptic curve cryptosystem techniques for encrypting the watermark before the embedding stage of digital watermarking process. As the combined version is used, it is very difficult for the attacker to extract the watermark. We have also seen that the PSNR values are more than +40dB; which indicates the robustness of the proposed algorithm. Similarly, the NC values show this algorithm is efficient enough to resists from the common attacks. The encryption and decryption times show the feasibility of the proposed algorithm. We have also used the ECC simulating with ElGamal for better security requirement, which encrypts ECC using ElGamal. This also, produces considerable results. Thus, we can conclude that when ever more security in the public domain is required for the watermark, we can use the combined version of 2D logistic map and elliptic curve cryptosystem or the combined version of 2D logistic map and elliptic curve cryptosystem simulating ElGamal.

REFERENCES

[1] Lu Ling, Sun Xinde, Cai Leiting, "A robust image watermarking based on DCT by Arnold transform and spread spectrum", IEEE International Conference on Advanced Computer Theory and Engineering, August 2010, vol. 1, pp. 198-201.

[2] Esam A. Hagras, M. S. El-Mahallawy, A. Zein Eldin, M. W. Fakhr, "Robust Secure and Blind Watermarking Based on DWT DCT Partial Multi Map Chaotic Encryption", International Journal of Multimedia and its Applications, November 2011, vol. 3, no. 4, pp. 37-47.

[3] Qingmei Wang, Fengyan Sun, Fengyu Liu, "Research on Public-Key Digital Watermarking System", IEEE International Conference on Communication Software and Networks, May 2011, pp. 158-162.

[4] Youssef Zaz, Lhoussain El Fadil, "Enhanced EPR Data Protection using Cryptography and Digital Watermarking", IEEE International Conference on Multimedia Computing and Systems, 2010, pp. 1-5.

[5] Hongbin Kong, Zhengquan Zeng, Lijun Yan, Jicheng Yang, Shaowen Yao , Nuoya Sheng, “Combine Elliptic Curve Cryptography with Digital Watermark for OWL- Based Ontology Encryption”, IEEE International Conference on Computational Intelligence and Security, 2009, pp. 511-515.
[6] Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang, Mengmeng Wang, “Digital Image Encryption Algorithm Based on Pixels”, IEEE International Conference on Intelligent Computing and Intelligent Systems, 2010, pp. 769-772.
[7] Chittaranjan Pradhan, Shibani Rath, Ajay Kumar Bisoi, “Non Blind Digital Watermarking Technique Using DWT and Cross Chaos”, Elsevier International Conference on Communication, Computing & Security, 2012, vol. 6, pp. 897-904.
[8] Qiang Wang, Qum Ding, Zhong Zhang, Lina Ding, “Digital Image Encryption Research Based on DWT and Chaos”, IEEE International Conference on Natural Computation, 2008 pp. 494-498.
[9] Musheer Ahmad and M. Shamsher Alam, “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping”, International Journal on Computer Science and Engineering, vol. 2(1), 2009, pp. 46-50.
[10] Behrouzan A. Forouzan, "Cryptography & Network Security", TMH Publisher, 2010, ISBN. 9780070660465.